

FILED

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

FEB 22 1 58 PM '96

RICHARD W. WIERING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA, S.J.

In the United States District Court
for the Northern District of California

ROGER SCHLAFLY, Plaintiff) Case C-94-20512 SW PVT
v.) Brief Regarding Stanford
PUBLIC KEY PARTNERS, and) Patent Validity
RSA DATA SECURITY INC., Defendants.) Feb. 29, 1996
San Jose

This brief supports the invalidity of the Stanford patents.

There are pending related motions in the above-captioned case, and in RSA Data v. Cylink/CKC, Case C-95-03256. Permission to file this brief was granted on Feb. 14, when the cases were partially consolidated, and an anticipatory letter was mailed to the parties on Feb. 15.

This brief addresses some points raised in the papers from the other case, and clarifies some issues.

1
2
3
4 Authorities
5

6 Carl Zeiss Stiftung v. Renishaw PLC, 945 F.2d 1173, 20 USPQ2d 1094,
7 (Fed Cir 1991).

8 In re Glass, 492 F.2d 1228, 181 USPQ 31 (CCPA 1974).

9 In re Wright, 999 F.2d 1557, 27 USPQ2d 1510 (Fed Cir 1993).

10 Newman v. Quigg, 877 F.2d 1575, 11 USPQ2d 1340 (Fed Cir 1989).

11 Patents, Donald Chisum.
12
13
14

15 Contents
16

17 Invalidity Issues Only

18 Distinct Position

19 Evidence

20 Printed Publication

21 Utility and Enablement

22 Trapdoor Knapsack Cracked

23 Conclusion
24
25
26
27
28

1 Invalidity Issues Only

2
3 For purposes of this brief, plaintiff Schlafly is operating under the
4 Court's order that the only issue which has been consolidated between
5 the two cases is the validity or invalidity of the Stanford patents.

6
7 If the Stanford patents are found to be valid, then there will
8 likely also be infringement issues which are common to the two
9 cases. However, Schlafly is not yet prepared to argue these
10 because: (1) infringement is not mentioned in any of the pending
11 motions in the instant case, (2) no infringement claims have been
12 detailed against Schlafly yet, (3) RSADSI's legal position is
13 significantly different because it has a patent license and is only
14 on the hook for contributory infringement, (4) a protective order
15 bars Schlafly from reviewing the papers regarding infringement in
16 the other case, and (5) the infringement issues are more
17 complicated, and Schlafly believes he can avoid them by proving
18 invalidity.

19
20 Therefore, Schlafly requests that infringement in the instant case
21 be argued later, if at all. When infringement issues are argued,
22 issues of claim construction and statutory subject matter can be
23 argued as well.

24
25 Distinct Position

26
27 At the start of this lawsuit, RSADSI was defending the Stanford
28 patents. Now RSADSI says they are invalid. Schlafly is happy to

1 have RSADSI on the same side of this particular issue, but notes
2 that their respective positions are not exactly the same.

3
4 Cylink/CKC argues that RSADSI should be barred by estoppel from
5 arguing invalidity. That argument rests on the fact that RSADSI was
6 a licensor of the Stanford patents. But there is no such bar against
7 Schlafly.

8
9 RSADSI has chosen not to make an invalidity argument based on
10 nonstatutory subject matter against the Stanford patents, because
11 such an argument would also knock out their own MIT patent. RSADSI
12 is probably also reluctant to argue inoperativeness, because its
13 Schnorr patent is expected to fall on similar grounds. Therefore,
14 the Court should draw no conclusion from RSADSI's failure to fully
15 support Schlafly's arguments.

16
17 Evidence

18
19 Evidence of patent invalidity that RSADSI has placed on the record
20 may properly be used in support of my motion. By announcing the
21 cases related, the Court has announced its intent to consider all of
22 the available evidence regarding the validity of the Stanford
23 patents. Evidence in the related case does indeed support my
24 motion.

25
26 Cylink/CKC had raised a question of admissibility of evidence, and
27 Schlafly contends that this issue has been resolved. (Cylink/CKC
28 argued at the Dec. 6, 1995 hearing that the Stanford validity issues

1 are now purely matters of law.) Regardless, RSADSI has filed
2 affidavits making all of the necessary Diffie-Hellman and Hellman-
3 Merkle evidence admissible.

4
5 Printed Publication

6
7 Cylink/CKC relies heavily on a literal interpretation of the term
8 "printed publication" in 35 USC 102(b). The term was introduced by
9 the 1836 patent law, and has not been changed. The term now seems
10 rather quaint in the light of all the technologies used to
11 communicate modern research. The courts have instead focussed on
12 whether there was an enabling disclosure which was accessible to the
13 public before the critical date. If there was such a disclosure,
14 recent courts have always invalidated the patent.

15
16 The record shows that the Diffie-Hellman inventors gave three public
17 lectures describing their invention more than one year prior to
18 filing the patent application. (Two were at conferences open to
19 anyone who paid the fee; one was a non-confidential lecture at IBM,
20 which was the major center of non-government cryptological activity
21 at the time.) The record also shows that the disclosure was
22 enabling. Cylink/CKC offers no evidence to the contrary, but merely
23 relies on a narrow interpretation of "printed publication".

24
25 While disclosure of some complicated inventions might not be
26 enabling based on an oral lecture or a slide show, the Diffie-
27 Hellman invention has a striking simplicity that allows it to be
28 described in a single slide or a few sentences.

1 In addition to the oral disclosures, the inventors distributed
2 preprints which qualify under the literal meaning of "printed
3 publication" anyway. There seems to be some confusion about the
4 meaning of "preprint". Webster's Collegiate Dictionary defines it
5 as "an issue of a technical paper often in preliminary form before
6 its publication in a journal". Academic researchers commonly
7 distribute preprints to whomever they can as soon as the manuscript
8 is submitted to a journal or presented at a conference. Usually the
9 preprint is just a xerox or laserprinted copy of the submitted
10 manuscript.

11
12 Thus, Schlafly produced proof of four enabling disclosures of the
13 Diffie-Hellman invention before the critical date. Three were
14 public lectures, and one was a distributed preprint. Contrary to
15 Cylink/CKC's assertion, the PTO was not informed of these four
16 disclosures. The PTO was informed of publication of the NCC and
17 "New Directions" papers. The former was determined to be not
18 enabling, because it did not disclose exponential key exchange. The
19 examiner did not know that exponential key exchange was disclosed in
20 the NCC lecture. The latter was not considered to be prior art
21 because the examiner only knew of submission and publication in the
22 IEEE journal, and did not know the preprint was distributed to the
23 public in August 1976.

24
25 Cylink/CKC tries to poke holes in the 35 USC 102(b) invalidity
26 argument, but common sense supports the argument. The inventors had
27 a hot result, and they knew it. They believed it would
28 revolutionize communications, and they spread the word with

1 missionary zeal. (Their "New Directions" preprint starts with the
2 sentence "We stand today on the brink of a revolution in
3 cryptography.") Within 2 months of their invention, they had
4 submitted a enabling paper to the IEEE journal and had given three
5 enabling public lectures to experts in the field. Nothing was
6 marked confidential and they were clearly not being the slightest
7 bit secretive about their invention. Their preprint was dated
8 August 1976 and the critical date was Sept. 6, 1976. We don't know
9 exactly how many copies were distributed before the critical date,
10 but at least one was and it seems extremely probable that anyone who
11 attended one of the lectures in June or July of 1976 who requested a
12 copy of the preprint would have received one before the critical
13 date. Therefore the August 1976 preprint should be considered a
14 printed publication, and so the 35 USC 102(b) statutory bar applies.

15 16 Utility and Enablement

17
18 A patentable invention must have utility. 35 USC 101. According to
19 the leading patent treatise, "To comply with the utility requirement
20 ... First, it must be operable and capable of use. It must operate
21 to perform the functions and secure the result intended." [Chisum,
22 4.01] For a recent case supporting this view, see Carl Zeiss
23 Stiftung v. Renishaw PLC, 945 F.2d 1173, 1180, 20 USPQ2d 1094, 1100
24 (Fed Cir 1991). At issue is whether post-filing art may be used to
25 prove lack of utility.

26
27 Closely related is the enablement requirement. 35 USC 112. "It is
28 apparent that lack of utility because of inoperativeness, and

1 absence of enablement, are closely related grounds of
2 unpatentability." Newman v. Quigg, 877 F.2d 1575, 1581, 11 USPQ2d
3 1340, 1345 (Fed Cir 1989). The specification must teach to one of
4 ordinary skill in the relevant art how to make and use the invention
5 in question. [paraphrasing Chisum 7.05[3].] The relevant art is
6 art which is reasonably well-known at the filing date. "Sufficiency
7 must be judged as of the filing date." In re Glass, 492 F.2d 1228.
8 Cylink/CKC mistakenly relies on this principle to argue that
9 evidence about the breaking of the trapdoor knapsack should be
10 ignored.

11
12 To see Cylink/CKC's error, it is important to distinguish between
13 evidence which proves enablement, and that which disproves
14 enablement. The former must predate the filing date, but the latter
15 need not. All of the Cylink/CKC cases cited involve dating evidence
16 which favors enablement, not inoperativeness. Eg, In re Glass
17 only finds that an applicant could not rely on what occurred
18 in the art after his filing date.

19
20 A recent case which considers both kinds of evidence is In re
21 Wright, 999 F.2d 1557, 27 USPQ2d 1510 (Fed Cir 1993). Some patent
22 claims for a vaccine were denied for lack of an enabling
23 specification. The Court would only look at papers favoring
24 enablement which were published before the filing date, but cited an
25 article published five years later as evidence that undue
26 experimentation would have been required to practice the invention.
27 (This double standard may seem unfair or inconsistent, but it is the
28 law and there is a solid rational basis for it. The different

1 evidence serves different purposes. Evidence favoring enablement is
2 concerned with whether the specification teaches the invention, and
3 evidence against enablement concerns whether the claims describe the
4 invention. Applying the same rule to both types of evidence, as
5 Cylink/CKC suggests, would allow patents based on falsehoods just
6 because the falsehoods were believed at one time. See *In re Glass*,
7 *supra*, for another such paradox which works against the inventor.)

8
9 The Hellman-Merkle enablement situation is similar to *In re Wright*.
10 Five years after filing and publishing, cryptologists were still
11 trying to figure out ways to make the trapdoor knapsack work, and
12 publishing papers with the conclusion that it does not.

13
14 Also, *In re Wright* is similar to Hellman-Merkle in another respect.
15 Wright had a vaccine on an obscure chicken virus, but was really
16 trying to get a claim broad enough to cover a hypothetical vaccine
17 on the HIV (AIDS) virus. Likewise, Hellman-Merkle recites a
18 trapdoor knapsack algorithm, but Cylink/CKC is trying to use it to
19 cover all of public key cryptography. The Wright claims would not
20 have fared any better if someone had found an AIDS vaccine in the
21 meantime.

22
23 Trapdoor Knapsack Cracked

24
25 Cylink/CKC's alleged contradiction in Konheim's statements [Reply
26 Memorandum in support of Caro-Kann's motion for preliminary
27 injunction, p. 12, l. 4-11] is not a contradiction at all. The
28 general knapsack problem was (and still is) thought to be

1 computationally infeasible. However, the trapdoor knapsacks devised
2 by Hellman-Merkle are special versions of the general knapsack, and
3 have been shown to be insecure. Decryption is computationally
4 feasible.

5
6 One issue relates to whether a 1977 cryptosystem which was broken in
7 1983 could still have been considered secure in 1977. Cylink/CKC
8 argues in the affirmative based on the fuzzy english meaning of the
9 word "secure". But the Hellman-Merkle patent instead uses a more
10 precise mathematical definition in terms of "demonstrably infeasible
11 cryptanalytic time" of more than 1,000,000,000,000,000,000,000,
12 000,000 operations. This criterion was never met in 1977, even
13 though it was a few years later that everyone was convinced that the
14 condition was not met. Hence the cryptosystem was not secure in
15 1977.

16
17 It might seem that there is a factual dispute here -- after all,
18 Cylink/CKC states that the trapdoor knapsack was secure in 1977 and
19 Schlafly denies it (along with RSADSI's expert). The difference is
20 that in 1977 the trapdoor knapsack had a certain illusory security
21 which was based on the lack of published attacks. However, the PTO
22 rightfully rejects claims referring to others' lack of knowledge,
23 and the Hellman-Merkle examiner insisted on claim language using
24 terms like "computationally infeasible" which were defined
25 intrinsically. Whether or not an algorithm is computationally
26 infeasible to invert is a mathematical question whose answer is
27 independent of the dates the trapdoor knapsack attacks were
28 published. Thus, the trapdoor knapsack might have had some security

1 in 1977 against those ignorant of attacks, but it was not secure in
2 the sense of the word as described and claimed in the Hellman-Merkle
3 patent.

4
5 Cylink/CKC raises the possibility that some variant of the Hellman-
6 Merkle trapdoor knapsack might still be secure. This seems very
7 unlikely, in view of the evidence on the record that: (1) Merkle
8 paid off \$100 and \$1000 bets, (2) the consensus of the published
9 literature is that the trapdoor knapsack has been broken, (3)
10 exhibits give step-by-step instructions on how to break the various
11 variants the trapdoor knapsack, and (4) everyone who has considered
12 implementing the trapdoor knapsack has been convinced of its
13 insecurity, and abandoned it.

14
15 But even if there is such a secure variant, the Hellman-Merkle
16 patent still fails for lack of enablement. "Although not explicitly
17 stated in section 112, to be enabling, the specification of a patent
18 must teach those skilled in the art how to make and use the full
19 scope of the claimed invention without 'undue experimentation'." In
20 Re Wright, supra. The Hellman-Merkle specification certainly does
21 not teach a 1977 cryptologist how to practice a secure public key
22 cryptosystem. In fact, we have had nearly twenty years of undue
23 experimentation by many of the top experts in cryptology, and they
24 still cannot figure out a way to make the trapdoor knapsack secure.

25
26 Admittedly, the burden is on Schlafly (and RSADSI) to give clear and
27 convincing evidence that the invention is inoperative or nonenabled.
28 Nevertheless, it is notable that Cylink/CKC and its experts are

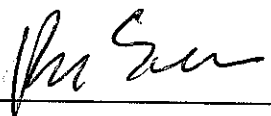
1 unable to point to any way of practicing the trapdoor knapsack
2 securely. The digital signature nonenablement is even more
3 embarrassing, as Cylink/CKC gives no way to practice it at all based
4 on the specification, much less practice it securely as required by
5 claims 4 and 5.

6
7 Therefore, the Hellman-Merkle patent is invalid for lack of utility
8 and enablement.

9
10 Conclusion

11
12 Schlafly believes that there are no material issues of fact in
13 dispute. The evidence strongly points to the invalidity of the
14 Stanford patents. A judicial declaration to that effect will
15 greatly simplify the cases at hand.

16
17
18 Dated: Feb 22, 1996

19
20 By: 

21
22 Plaintiff, Roger Schlafly, Pro Se